LA SETTIMANA CIBERNETICA

14 - 20 OTTOBRE 2024

18 OTTOBRE 2024

Campagna di smishing a tema Intesa Sanpaolo

(AL05/241018/CSIRT-ITA)

Questo CSIRT ha recentemente rilevato una campagna di smishing a tema Intesa Sanpaolo, perpetrata via SMS, volta a carpire le credenziali d'accesso ai servizi bancari.

LEGGI DI PIÙ →

18 OTTOBRE 2024

Aggiornamenti per VMware Spring

(AL04/241018/CSIRT-ITA)

Aggiornamenti di sicurezza VMware risolvono una vulnerabilità in Spring, noto framework open source per lo sviluppo di applicazioni Java. Tale vulnerabilità, qualora sfruttata, potrebbe permettere l'accesso ad informazioni sensibili presenti sui sistemi target.

CVE-2024-38819

LEGGI DI PIÙ →

18 OTTOBRE 2024

Risolta vulnerabilità in Grafana

(AL03/241018/CSIRT-ITA)

Rilasciati aggiornamenti di sicurezza per risolvere una vulnerabilità con gravità "critica" presente in Grafana, nota applicazione web per la visualizzazione e l'analisi interattiva di dati.

CVE-2024-9264

LEGGI DI PIÙ →

18 OTTOBRE 2024

Aggiornamenti per prodotti Trend Micro

(AL02/241018/CSIRT-ITA)

Sanate due vulnerabilità, di cui una con gravità "critica" e una con gravità "alta", realtivi a Cloud Edge e Deep Security Agent di Trend Micro. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato remoto di eseguire codice arbitrario o di elevare i propri privilegi sui sistemi target.

CVE-2024-48904 CVE-2024-48903

LEGGI DI PIÙ →

18 OTTOBRE 2024

Rilevate vulnerabilità in F5 BIG-IP

(AL01/241018/CSIRT-ITA)

Rilevate vulnerabilità, con gravità "alta", nei prodotti BIG-IP, piattaforma di servizi applicativi e di rete progettata per migliorare la disponibilità, la sicurezza e le prestazioni delle applicazioni web.

CVE-2024-45844

LEGGI DI PIÙ →

18 OTTOBRE 2024

Molteplici vulnerabilità in vari prodotti Veeam

(AL02/240906/CSIRT-ITA) - Aggiornamento

Veeam ha reso noto, tramite un bollettino di sicurezza, la presenza di molteplici vulnerabilità in alcuni dei suoi prodotti, di cui 5 con gravità "critica".

CVE-2024-40711 CVE-2024-40713 CVE-2024-40710 CVE-2024-39718 CVE-2024-40714 CVE-2024-40712
CVE-2024-40709 CVE-2024-42024 CVE-2024-42019 CVE-2024-42023 CVE-2024-42021 CVE-2024-42022
CVE-2024-42020 CVE-2024-38650 CVE-2024-39714 CVE-2024-39715 CVE-2024-38651 CVE-2024-40718

LEGGI DI PIÙ →

17 OTTOBRE 2024

Risolte vulnerabilità in Google Chrome

(AL05/241017/CSIRT-ITA)

Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere 17 vulnerabilità di sicurezza, di cui 1 con gravità “alta”.

CVE-2024-9954

LEGGI DI PIÙ →

17 OTTOBRE 2024

Vulnerabilità in Solarwinds Web Help Desk

(AL05/240814/CSIRT-ITA) - Aggiornamento

Risolte due vulnerabilità, con gravità “critica”, nel prodotto Web Help Desk di SolarWinds. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato l’esecuzione di codice arbitrario e la lettura/modifica di file sui dispositivi target.

CVE-2024-28986 CVE-2024-28987

LEGGI DI PIÙ →

17 OTTOBRE 2024

Aggiornamenti Mensili Microsoft

(AL01/240612/CSIRT-ITA) - Aggiornamento

Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 51 nuove vulnerabilità, di cui una di tipo 0-day.

CVE-2024-30087	CVE-2024-30052	CVE-2024-30084	CVE-2024-30065	CVE-2024-30067	CVE-2024-35263
CVE-2024-35249	CVE-2024-30074	CVE-2024-35252	CVE-2024-37325	CVE-2024-29187	CVE-2024-30069
CVE-2024-30091	CVE-2024-30101	CVE-2024-30104	CVE-2024-30077	CVE-2024-30066	CVE-2024-35253
CVE-2024-35254	CVE-2024-30083	CVE-2024-30072	CVE-2023-50868	CVE-2024-30095	CVE-2024-30088
CVE-2024-30075	CVE-2024-30062	CVE-2024-30097	CVE-2024-30076	CVE-2024-30064	CVE-2024-30103
CVE-2024-30070	CVE-2024-30094	CVE-2024-30102	CVE-2024-35248	CVE-2024-30089	CVE-2024-30100
CVE-2024-30082	CVE-2024-35265	CVE-2024-30078	CVE-2024-30096	CVE-2024-30085	CVE-2024-35250
CVE-2024-30090	CVE-2024-30063	CVE-2024-30080	CVE-2024-35255	CVE-2024-30068	CVE-2024-30093
CVE-2024-29060	CVE-2024-30086	CVE-2024-30099			

LEGGI DI PIÙ →

17 OTTOBRE 2024

Aggiornamenti Drupal

(AL04/241017/CSIRT-ITA)

Aggiornamenti di sicurezza risolvono una vulnerabilità, con gravità “alta”, in Drupal. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di compromettere la disponibilità del servizio sui sistemi target.

LEGGI DI PIÙ →

17 OTTOBRE 2024

Risolte vulnerabilità in prodotti Cisco

(AL03/241017/CSIRT-ITA)

Aggiornamenti di sicurezza sanano 10 nuove vulnerabilità, di cui 2 con gravità “alta”, in alcuni prodotti Cisco.

CVE-2024-20421 CVE-2024-20458

LEGGI DI PIÙ →

17 OTTOBRE 2024

Rilevata vulnerabilità in Image Builder per Kubernetes

(AL02/241017/CSIRT-ITA)

Rilevata una vulnerabilità, con gravità “critica”, nel prodotto Kubernetes Image Builder, in cui le credenziali di default sono abilitate durante il processo di compilazione dell’immagine. Tale vulnerabilità potrebbe consentire l’elevazione dei privilegi e/o il bypass dei meccanismi di autenticazione.

CVE-2024-9486

LEGGI DI PIÙ →

17 OTTOBRE 2024

Rilevata vulnerabilità in prodotti VMware

(AL01/241017/CSIRT-ITA)

VMware ha rilasciato un aggiornamento di sicurezza per sanare una vulnerabilità, con gravità “alta”, in VMware HCX.

CVE-2024-38814

LEGGI DI PIÙ →

16 OTTOBRE 2024

Vulnerabilità in prodotti Solarwinds

(AL03/241016/CSIRT-ITA)

Risolte 6 vulnerabilità di sicurezza, di cui 3 con gravità “alta” una con gravità “critica”, in vari prodotti SolarWinds.

CVE-2024-45715 CVE-2024-45710 CVE-2024-45711 CVE-2024-28988

LEGGI DI PIÙ →

16 OTTOBRE 2024

Critical Patch Update di Oracle

(AL02/241016/CSIRT-ITA)

Oracle ha rilasciato il Critical Patch Update di ottobre che descrive 334 vulnerabilità su più prodotti, di cui 16 con gravità "critica". Tra queste, alcune potrebbero essere sfruttate per eseguire operazioni non autorizzate oppure compromettere la disponibilità del servizio sui sistemi target.

CVE-2022-46337 CVE-2024-45492 CVE-2023-38408 CVE-2024-4577 CVE-2023-6816 CVE-2022-2068
CVE-2022-34381 CVE-2024-21216 CVE-2022-23305 CVE-2023-38545 CVE-2024-28752 CVE-2024-37371
CVE-2024-29736 CVE-2024-5535 CVE-2022-36760 CVE-2024-21172

LEGGI DI PIÙ →

16 OTTOBRE 2024

Mozilla: vulnerabilità relativa al browser Firefox

(AL01/241016/CSIRT-ITA)

Mozilla ha rilasciato aggiornamenti di sicurezza per correggere una vulnerabilità con gravità "alta" nel noto browser Firefox, che qualora sfruttata potrebbe comportare la compromissione della disponibilità del servizio.

CVE-2024-9936

LEGGI DI PIÙ →

15 OTTOBRE 2024

Rilevate vulnerabilità in prodotti Splunk

(AL01/241015/CSIRT-ITA)

Splunk ha rilasciato aggiornamenti di sicurezza per correggere alcune vulnerabilità, di cui 3 con gravità "alta", nei noti prodotti per l'analisi del traffico di rete Enterprise e Cloud Platform.

CVE-2024-45731 CVE-2024-45732 CVE-2024-45733

LEGGI DI PIÙ →

14 OTTOBRE 2024

Sanate vulnerabilità in Apache OFBiz

(AL02/240904/CSIRT-ITA) - Aggiornamento

Risolte due vulnerabilità, di cui una con gravità "alta", nel prodotto OFBiz di Apache Software Foundation. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato l'esecuzione di codice arbitrario sui sistemi interessati e l'accesso a informazioni sensibili.

CVE-2024-45507 CVE-2024-45195

LEGGI DI PIÙ →

14 OTTOBRE 2024

Aggiornamenti Mensili Microsoft

(AL01/241009/CSIRT-ITA) - Aggiornamento

Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 120 nuove vulnerabilità, di cui 5 di tipo 0-day.

CVE-2024-43543	CVE-2024-43546	CVE-2024-43456	CVE-2024-43483	CVE-2024-37983	CVE-2024-43564
CVE-2024-38212	CVE-2024-43575	CVE-2024-43521	CVE-2024-43612	CVE-2024-43523	CVE-2024-43535
CVE-2024-38265	CVE-2024-43582	CVE-2024-43506	CVE-2024-43589	CVE-2024-43583	CVE-2024-43574
CVE-2024-43497	CVE-2024-43503	CVE-2024-43513	CVE-2024-43611	CVE-2024-43488	CVE-2024-43552
CVE-2024-43570	CVE-2024-43556	CVE-2024-43547	CVE-2024-43593	CVE-2024-43524	CVE-2024-43516
CVE-2024-43554	CVE-2024-43544	CVE-2024-43485	CVE-2024-43533	CVE-2024-43522	CVE-2024-43542
CVE-2024-43615	CVE-2024-43551	CVE-2024-43555	CVE-2024-27397	CVE-2024-43536	CVE-2024-43608
CVE-2024-43614	CVE-2024-43515	CVE-2024-38262	CVE-2024-43541	CVE-2024-43581	CVE-2024-43565
CVE-2024-43601	CVE-2024-38179	CVE-2024-30092	CVE-2024-43529	CVE-2024-43520	CVE-2024-38097
CVE-2024-43538	CVE-2024-43567	CVE-2024-43504	CVE-2024-38229	CVE-2024-43572	CVE-2024-43484
CVE-2024-38124	CVE-2024-6197	CVE-2024-43591	CVE-2024-43500	CVE-2024-37982	CVE-2024-43532
CVE-2024-43519	CVE-2024-43610	CVE-2024-43573	CVE-2024-43518	CVE-2024-43480	CVE-2024-43604
CVE-2024-43562	CVE-2024-43468	CVE-2024-43549	CVE-2024-43557	CVE-2024-37979	CVE-2024-43509
CVE-2024-43540	CVE-2024-43603	CVE-2024-43528	CVE-2024-43571	CVE-2024-43560	CVE-2024-43517
CVE-2024-43558	CVE-2024-43616	CVE-2024-43563	CVE-2024-43585	CVE-2024-43534	CVE-2024-43453
CVE-2024-43584	CVE-2024-43501	CVE-2024-43505	CVE-2024-43527	CVE-2024-43559	CVE-2024-38029
CVE-2024-43599	CVE-2024-43607	CVE-2024-43592	CVE-2024-38129		

LEGGI DI PIÙ →

14 OTTOBRE 2024

Aggiornamenti di sicurezza Apple

(AL01/240917/CSIRT-ITA) - Aggiornamento

Apple ha rilasciato aggiornamenti di sicurezza per sanare molteplici vulnerabilità presenti nei propri prodotti.

CVE-2024-40840	CVE-2024-40830	CVE-2024-44171	CVE-2024-40852	CVE-2024-27874	CVE-2024-27876
CVE-2024-27869	CVE-2024-44124	CVE-2024-44131	CVE-2024-40850	CVE-2024-27880	CVE-2024-44176
CVE-2024-44169	CVE-2024-44165	CVE-2024-44191	CVE-2024-44198	CVE-2024-40791	CVE-2024-44183
CVE-2023-5841	CVE-2024-44147	CVE-2024-44167	CVE-2024-40826	CVE-2024-44202	CVE-2024-44127
CVE-2024-40863	CVE-2024-44139	CVE-2024-44180	CVE-2024-44170	CVE-2024-44184	CVE-2024-27879
CVE-2024-40857	CVE-2024-44187	CVE-2024-40856	CVE-2024-44129	CVE-2024-44153	CVE-2024-44188
CVE-2024-40825	CVE-2024-44130	CVE-2024-44182	CVE-2024-44154	CVE-2024-40845	CVE-2024-40846
CVE-2024-44164	CVE-2024-40837	CVE-2024-40847	CVE-2024-40848	CVE-2024-44168	CVE-2024-27860
CVE-2024-27861	CVE-2024-40841	CVE-2024-27795	CVE-2024-44135	CVE-2024-44132	CVE-2024-44128
CVE-2024-44151	CVE-2024-27875	CVE-2024-44146	CVE-2023-4504	CVE-2024-44148	CVE-2024-44177
CVE-2024-40831	CVE-2024-40861	CVE-2024-44160	CVE-2024-44161	CVE-2024-44181	CVE-2024-27858
CVE-2024-40838	CVE-2024-44186	CVE-2024-39894	CVE-2024-44178	CVE-2024-44149	CVE-2024-40797
CVE-2024-44125	CVE-2024-44163	CVE-2024-40801	CVE-2024-44158	CVE-2024-40844	CVE-2024-40860
CVE-2024-44152	CVE-2024-44166	CVE-2024-44190	CVE-2024-44133	CVE-2024-40859	CVE-2024-41957
CVE-2024-40866	CVE-2024-40770	CVE-2024-23237	CVE-2024-44134	CVE-2024-44189	CVE-2024-40842
CVE-2024-40843	CVE-2024-40790	CVE-2024-44162	CVE-2024-40862	CVE-2024-27886	CVE-2024-40814

LEGGI DI PIÙ →

14 OTTOBRE 2024

Aggiornamenti per VMware Spring

(AL02/240913/CSIRT-ITA) - Aggiornamento

Aggiornamenti di sicurezza VMware risolvono una vulnerabilità in Spring, noto framework open source per lo sviluppo di applicazioni Java. Tale vulnerabilità, qualora sfruttata, potrebbe permettere l'accesso ad informazioni sensibili presenti sui sistemi target.

CVE-2024-38816

LEGGI DI PIÙ →

14 OTTOBRE 2024

Mozilla: rilevato sfruttamento in rete della CVE-2024-9680

(AL03/241010/CSIRT-ITA) - Aggiornamento

Rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-9680 – già sanata dal vendor – che interessa i noti prodotti: Firefox e Thunderbird. Tale vulnerabilità, di tipo "Use-After-Free", che interessa la componente timeline delle animazioni di tali prodotti.

CVE-2024-9680

LEGGI DI PIÙ →